



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,448	04/27/2006	Masao Nonaka	2006_0611A	4794
52349 7590 12/28/2009 WENDEROTH, LIND & PONACK L.L.P. 1030 15th Street, N.W. Suite 400 East Washington, DC 20005-1503				
EXAMINER				
POPHAM, JEFFREY D				
ART UNIT		PAPER NUMBER		
2437				
MAIL DATE		DELIVERY MODE		
12/28/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/577,448

Applicant(s)

NONAKA ET AL.

Examiner

JEFFREY D. POPHAM

Art Unit

2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 October 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1, 3-10, 27-29 and 34 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 3-10, 27-29 and 34 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 April 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Remarks

Claims 1, 3-10, 27-29, and 34 are pending.

Response to Arguments

1. Applicant's arguments filed 10/28/2009 have been fully considered but they are not persuasive.

Applicant argues that the present invention "is clearly different from Nakano in that (in the present invention) the node encryption key group is selected such that the encryption key group includes the node encryption key in the terminal node." However, Nakano provides for key groups that are used to encrypt content decryption keys, wherein such key groups will include multiple keys. As an example, page 51, lines 9-13 state that an encryption key group is formed using 3 encryption keys (0-1K1000, 1-1K1000, and 2-1K1000). As can be seen in page 43, each terminal is assigned 22 keys. Each of these 22 keys corresponds to the "node encryption key that is set for the selected terminal node" as each one is set for that particular terminal node. One can get a clear understanding of the description on page 51 from figure 15. The 3 keys that are being used are at levels 0, 1, and 2. The first key (0-1K1000) is set for terminals 17 and higher. The second key (1-1K1000) is set for terminals 5-16 (although not shown on the figure, these are the terminals that would be under the level 2 nodes 2, 3, and 4. The final key (2-1K1000) is set for terminals 2-4. Clearly, this key group "includes a node encryption key that is set for the selected terminal node and a node encryption key that is set for a node other than the selected

Art Unit: 2437

terminal node", where the selected terminal node may be any of the nodes, as all valid nodes are taken into consideration when creating this key group, so as to provide all valid nodes with an appropriate representation of the decryption key.

Further description as to this teaching could be found with reference to figure 21, and the corresponding description. In pertinent part, page 69, lines 1-4 describes a group that includes seven encryption keys. These encryption keys include 1-1K1000, 1-2K1000, 1-3K0000, 1-4K0000, 2-5K1000, 3-3K, and 3-4K. As one can see, these seven keys can be used to encrypt the content decryption key such that all but the revoked terminals can decrypt the decryption key. Furthermore, this setup uses keys from levels 1, 2, and 3. Therefore, keys 3-3K and 3-4K are each specific to a single terminal. These terminals must be selected in the creation of the group in order to designate the keys for them. Therefore, terminal 3 is selected during creation of the key group, and the key group includes the specific key for terminal 3, the specific key for terminal 4, and keys set in all of terminals 5-16 and 18-64. At least the above described examples clearly and explicitly disclose "said encryption key group selection unit selects at least one terminal node from among the terminal nodes, and selects the selected node encryption key group so that the selected node encryption key group includes a node encryption key that is set for the selected terminal node and a node encryption key that is set for a node other than the selected terminal node."

Specification

2. The disclosure is objected to because of the following informalities: Page 10, lines 8-12 read "It should also be noted that such programs can not only be stored in a ROM and the like incorporated into the content distribution server, the content output apparatus and the key issuing center, but also be distributed on a recording medium such as a CD-ROM and via a communication network." It appears as though Applicant intends for a communication network to be distinct from a recording medium, however, it is not clearly specified here. As currently described, examples of a recording medium may be interpreted to include a CD-ROM and a communication network. If Applicant intends for a recording medium to include a communication network, 101 issues will arise with respect to claim 29. However, if Applicant intends for a communication network to be distinct from a recording medium (as the Examiner believes to be the case), the following amendment is suggested to the above-cited portion of the disclosure. The portion reading "but also could be distributed on a recording medium such as a CD-ROM and via a communication network" could be switched, such that it reads "but also could be distributed via a communication network or on a recording medium such as a CD-ROM".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to

Art Unit: 2437

be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 3-10, 29, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakano (WO 02/078419 A2) in view of Lao (U.S. Patent 7,343,324).

Regarding Claim 1,

Nakano discloses a content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the content distribution server (encryption device, for example) comprising:

A key information storage unit operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method (Page 29, lines 8-22; encryption key group storage unit storing keys and key designation information received from key setting system);

An encryption key group selection unit operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group (Page 22, line 8 to Page 23, line 11; deciding and selecting keys to be used);

A content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using the at least one node encryption key in the selected node encryption key group (Page 29, lines 4-7 and 23-27; key encryption unit encrypted the generated content key using each stored/selected encryption key);

An encryption unit operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key (Page 29, line 28 to Page 30, line 3; content encryption unit encrypting the content with the content key; one will note that the instant application states that "A content encryption key CEK and a corresponding content decryption key may have the same value" (Page 42, lines 14-15). Therefore, even in embodiments of Nakano in which the keys are symmetric, the symmetric key clearly reads on the combination of encryption key and decryption key); and

A transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the content output apparatuses (Page 30, lines 4-10; and Page 74, line 23 to Page 75, line 14; the output unit employing transmission across transmission paths);

That the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

Classifying the nodes into a plurality of levels from a 0th level through an nth level, n being 1 or a larger natural number (Figure 4; and Page 33, lines 7-17; showing a 4-ary tree);

Selecting, as terminal nodes in the tree structure, nodes each of which does not have a child node, from among the nodes (Figure 4; Page 33, lines 7-17; and Page 35, line 26 to Page 36, line 3; showing terminals as being leaves, as well as the possibility that not every lowest-level node will be associated with a terminal, therefore, providing for leaf nodes that are not on the lowest level); and

The encryption key group selection unit selects at least one terminal node from among the terminal nodes, and selects the selected node encryption key group so that the selected node encryption key group includes a node encryption key that is set for the selected terminal node and a node encryption key that is set for a node other than the selected terminal node (Figures 11, 15, and 21; Page 43, lines 3-25; Page 51, lines 9-13; Page 66, lines 3-18; and Page 69, lines 1-4; for example, showing keys set in valid terminals being set as the key group, such keys including keys from

the root layer (in figure 15) to the leaf/terminal layer (in figure 21), for example);

But does not explicitly disclose a content receiving unit operable to receive a content via the network.

Lao, however, discloses a content receiving unit operable to receive a content via the network (Figure 7; Column 1, lines 8-12; Column 6, lines 31-36; Column 7, lines 63-67; and Column 9, lines 61-67; the distributor receiving content over a network). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content publishing system of Lao into the data protection system of Nakano in order to allow the creators of content to specify the rights that may be allowed for a particular piece of content before allowing the content to be distributed, thereby ensuring proper control for content creators.

Regarding Claim 29,

Claim 29 is a program claim that corresponds to server claim 1 and is rejected for the same reasons.

Regarding Claim 34,

Claim 34 is a method claim that corresponds to server claim 1 and is rejected for the same reasons.

Regarding Claim 3,

Nakano as modified by Lao discloses the server of claim 1, in addition, Nakano discloses that the tree structure in the key

assignment method is an N-ary tree, N being 2 or a larger natural number (Figure 4; showing a 4-ary tree).

Regarding Claim 4,

Nakano as modified by Lao discloses the server of claim 1, in addition, Nakano discloses a content key generation unit operable to newly generate at least one pair of a content encryption key and a corresponding content decryption key which is different from at least one pair of a content encryption key which is previously used for encrypting a content and a corresponding content decryption key, in the case where the content receiving unit receives a new content (Page 29, lines 4-7; and Page 29, line 23 to Page 30, line 3; randomly generating the content key).

Regarding Claim 5,

Nakano as modified by Lao discloses the server of claim 1, in addition, Nakano discloses that the encryption key group selection unit newly selects a selected node encryption key group including a node encryption key that is set for another terminal node than a previously selected terminal node, in the case of receiving a new content via the content receiving unit (Figures 14 and 15; Page 22, line 8 to Page 23, line 11; Page 48, line 24 to Page 49, line 3; and Page 51, lines 9-13; showing that content may, at first, be sent using the key 0-1K0000, which is held by all decryption devices; the invalidation of device 1; and the use of keys

0-1K1000, 1-1K1000, and 2-1K1000 in encrypting keys for later provided content, such that device 1 cannot access the content, since it has no keys that can be used to decrypt the content key).

Regarding Claim 6,

Nakano as modified by Lao discloses the server of claim 1, in addition, Nakano discloses a key selection information storage unit operable to hold a plurality of key selection information which are used for selecting the node encryption key included in the node encryption key group (Page 29, lines 8-22; storage of key designation information);

Wherein the encryption key group selection unit selects the selected node encryption key group based on the key selection information (Page 22, line 8 to Page 23, line 11; and Page 29, lines 8-22; selecting keys using the key designation information).

Regarding Claim 7,

Nakano as modified by Lao discloses the server of claim 6, in addition, Nakano discloses that the key selection information storage unit further holds a plurality of key selection identifiers that identify the key selection information, the key selection identifiers and the key selection information being associated with each other (Figure 16; and Page 51, line 23 to Page 52, line 7; showing the format of key designation information including a node ID);

The encryption key group selection unit selects the selected node encryption key group based on the key selection information (Page 22, line 8 to Page 23, line 11; and Page 29, lines 8-22); and

The transmission unit distributes, to the content output apparatuses, the encrypted content, the encrypted content key decryption key, and the key selection identifiers associated with the key selection information (Page 74, line 23 to Page 75, line 14; showing transmission of encrypted content, encrypted content key, and key designation information).

Regarding Claim 8,

Nakano as modified by Lao discloses the server of claim 6, in addition, Nakano discloses that the encryption key group selection unit selects, on a random basis, one of the key selection information from among the plurality of key selection information held in the key selection information storage unit, and selects the selected node encryption key group based on the selected key selection information (Page 22, line 8 to Page 23, line 11; the arbitrary setting of two or more terminal groups, as well as the selection of keys for each terminal and each terminal group. This all appears to be performed in a non-structured (e.g. random) basis, as groups can overlap and multiple groups can contain the same device, therefore, the groups must be selected "on a random basis". Further randomness is found in checking for keys

corresponding to invalid terminals, such invalid terminals being randomly distributed throughout the terminals and/or groups).

Regarding Claim 9,

Nakano as modified by Lao discloses the server of claim 6, in addition, Nakano discloses that the key group selection unit selects, at regular intervals, one of the key selection information from among the plurality of key selection information held in the key selection information storage unit, and selects the selected node encryption key group based on the selected key selection information (Page 22, line 8 to Page 23, line 11; Page 48, line 24 to Page 49, line 3; and Page 51, lines 9-13; showing selecting the key groups; such selection being done at regular intervals. In this case, the interval is between distribution of each piece of content, when the key groups are selected, for example).

Regarding Claim 10,

Nakano as modified by Lao discloses the server of claim 1, in addition, Nakano discloses a storage unit operable to store the node encryption key group received via the network into the key information storage unit (Page 29, lines 8-22; storing key groups that have been received from the key setting system).

Art Unit: 2437

4. Claims 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakano in view of Lao and Asano (U.S. Patent Application Publication 2003/0051151).

Regarding Claim 27,

Nakano discloses a content distribution system comprising content output apparatuses, and a content distribution server, each of the content output apparatuses decrypting an encrypted content using a content decryption key and outputting the decrypted content, and a content distribution server creating an encrypted content by encrypting the content, and distributing the encrypted content to each content output apparatus via a network:

Wherein the content output apparatus includes:

A first receiving unit operable to receive the encrypted content and an encrypted content decryption key group which are distributed from the content distribution server (Page 31, lines 3-9; and Page 74, line 23 to Page 75, line 14);

A node key storage unit operable to hold the node decryption key group (Page 31, lines 10-15);

A decryption key obtaining unit operable to obtain the content decryption key based on at least one node decryption key group and at least one encrypted content decryption key group (Page 31, lines 22-26); and

A first decryption unit operable to decrypt the encrypted content using the content decryption key (Page 31, line 27 to Page 32, line 3); and

The content distribution server includes:

A key information storage unit operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method (Page 29, lines 8-22);

An encryption key group selection unit operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group (Page 22, line 8 to Page 23, line 11);

A content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using the at least one node encryption key in the selected node encryption key group (Page 29, lines 4-7 and 23-27);

An encryption unit operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key (Page 29, line 28 to Page 30, line 3); and

A transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the

content output apparatuses (Page 30, lines 4-10; and Page 74, line 23 to Page 75, line 14);

That the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

Classifying the nodes into a plurality of levels from a 0th level through an nth level, n being 1 or a larger natural number (Figure 4; and Page 33, lines 7-17);

Selecting, as terminal nodes in the tree structure, nodes each of which does not have a child node, from among the nodes (Figure 4; Page 33, lines 7-17; and Page 35, line 26 to Page 36, line 3); and

The encryption key group selection unit selects at least one terminal node from among the terminal nodes, and selects the selected node encryption key group so that the selected node encryption key group includes a node encryption key that is set for the selected terminal node and a node encryption key that is set for a node other than the selected terminal node (Figures 11, 15, and 21; Page 43, lines 3-25; Page 51, lines 9-13; Page 66, lines 3-18; and Page 69, lines 1-4);

But does not explicitly disclose a content receiving unit operable to receive a content via the network; or a second receiving unit operable to receive, via the network, a node decryption key

group which is previously assigned by a predetermined key assignment method.

Lao, however, discloses a content receiving unit operable to receive a content via the network (Figure 7; Column 1, lines 8-12; Column 6, lines 31-36; Column 7, lines 63-67; and Column 9, lines 61-67). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content publishing system of Lao into the data protection system of Nakano in order to allow the creators of content to specify the rights that may be allowed for a particular piece of content before allowing the content to be distributed, thereby ensuring proper control for content creators.

Asano, however, discloses a second receiving unit operable to receive, via the network, a node decryption key group which is previously assigned by a predetermined key assignment method (Paragraphs 181-183). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the key updating techniques of Asano into the data protection system of Nakano as modified by Lao in order to allow the system to dynamically update key groups when desired, thereby forcefully removing invalid devices from the system by halting storage and usage of any of the keys held by such invalid devices, thereby providing for forward secrecy, while allowing for

periodic key updates such that, even if various keys used in the system are hacked, they will not be usable after such update, thereby further securing the system.

Regarding Claim 28,

Nakano as modified by Lao and Asano discloses the system of claim 27, in addition, Asano discloses a key issuing center that is connected, via a network, with the content distribution server and the content output apparatuses, and issues a key for obtaining a content decryption key to each of the content output apparatuses, wherein the key issuing center includes:

A node key generation unit operable to generate, based on a predetermined key assignment method, a node encryption key group that is a set of node encryption keys and a node decryption key group that is a set of node decryption keys, each of the node encryption keys and node decryption keys being assigned to each content output apparatus (Page 33, lines 7-17; Page 34, lines 4-16; and Page 38, lines 10-15);

A first transmission unit operable to transmit the node encryption key group to the content distribution server (Page 34, line 17 to Page 35, line 4);

A node decryption key group selection unit operable to select at least one of the node decryption keys, and generate the

node decryption key group to be distributed to each content output apparatus (Page 34, lines 4-16); and

A transmission unit operable to distribute the node decryption key group to a manufacturing system for storage in the content output apparatus (Page 34, lines 4-16); and

Asano discloses a second transmission unit operable to distribute the node decryption key group to the content output apparatus (Paragraphs 181-183).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone

Art Unit: 2437

number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437